UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,409	01/16/2004	Luciano M. Silva	RSW920030258US1 (140)	7485

46320 7590 02/20/2008

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
PARK, JEONG S	

ART UNIT	PAPER NUMBER
2154	

MAIL DATE	DELIVERY MODE
02/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/759,409	SILVA, LUCIANO M.	
	Examiner	Art Unit	
	Jeong S. Park	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to communications filed December 4, 2007.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 4 and 6-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bazinet et al. (hereinafter Bazinet)(U.S. Pub. No. 2003/0167298 A1), and further in view of Vasandani et al. (hereinafter Vasandani)(U.S. Patent No. 6,985,946 B1).

Regarding claim 4, Bazinet teaches as follows:

a system for programmatic role-based security in a dynamically generated user interface, the system comprising:

an application framework configured through a deployment descriptor (portal generic objects database) comprising a listing of a set of views (n generic objects 204 in figure 2, each object creates different view), a listing of associated program logic (based on the access privileges of the authenticated user the database lists different access level) and a listing of a set of authorized actions (read, read/write, or no access, 208 in figure 2, indicates the roles) for selected ones of said views (see, e.g., page 2, paragraph [0030]);

a first view (502 in figure 5) listed in said deployment descriptor (portal generic

objects database) and comprising a linkage to a second view (linkage to the backend applications 126 in figure 1) listed in said deployment descriptor (the portal application generates a page to the client containing entries corresponding to the backend applications that the authenticated user can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraphs [0038] and figure 5); and

access checking logic disposed in said first view and programmed to omit said linkage (no access) where a role of an end user accessing said first view is not authorized to access said second view according to said listing of said set of authorized roles in said deployment descriptor (the instructions, 506 in figure 5, only shows what are authorized to the client, see, e.g., page 4, paragraph [0040] and figure 5).

Bazinet does not teach the security control by user roles.

Vasandani teaches as follows:

providing role based access security within a networked computing system (see, e.g., col. 2, lines 40-43); and

the method for providing an authentication and authorization pipeline having a userID-roles database and a resource-roles database for use in a web server to grant access to web resources to users (see, e.g., col. 2, line 58 to col. 3, line 9).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claim 6, Bazinet teaches as follows:

said program logic comprises servlets and wherein said views comprise Java server pages (the Web page sent by the portal server to the clients may include Java server pages, see, e.g., page 2, paragraph [0026], lines 12-17).

Regarding claim 7, Bazinet teaches as follows:

a custom tag (instructions 506 in figure 5, see, e.g., page 4, paragraph [0039]) disposed in said first view for invoking said access checking logic and for omitting said linkage responsive to said access checking logic (the first Web page shows the instruction tag for users to select eligible applications based on the access privileges of the authenticated user, see, e.g., page 3, paragraph [0030] and [0038]).

Regarding claim 8 and 12, Bazinet teaches as follows:

a method for programmatic user privilege based security in a dynamically generated user interface (see, e.g., abstract), the method comprising the steps of:

authenticating access to a rendering of a selected view based upon an end user's privileges (access privileges of the authenticated user) requesting access to said selected view (see, e.g., step 414 in figure 4 and page 3, paragraph [0037]);

processing said selected view to identify a method call to access checking logic (see, e.g., steps 422-434 in figure 4 and page 4, paragraphs [0042]-[0044]); and

disposing a link to said different view in said rendering of said selected view conditional upon said role matches a role in said set of roles (the privilege stored in the portal generic objects database)(the portal application generate a page to the client containing entries corresponding to the backend applications that the authenticated user

can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraph [0038] and step 416 in figure 4).

Bazinet does not teach role based security access and following steps of using it but all limitations with user's privilege based security access.

Vasandani teaches as follows:

providing role based access security within a networked computing system (see, e.g., col. 2, lines 40-43);

the method for providing an authentication and authorization pipeline having a userID-roles database and a resource-roles database for use in a web server to grant access to web resources to users (see, e.g., col. 2, line 58 to col. 3, line 9); and

comparing said role (userID-roles object, 211 in figure 4) to a set of roles (roles/access database, 422 in figure 4) authorized to access a different view (requested resource) associated with said access checking logic (the roles authorization module retrieves the database entry for the requested resource using the URI and attempts to match a role from the userID-roles object with the roles in the roles/access database entry, see, e.g., col. 8, lines 1-4).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claims 9-11 and 13-15, Vasandani teaches as follows:

said step of authenticating comprises the step of comparing said role (userID-roles object, 211 in figure 4) to a set of roles (roles/access database, 422 in figure 4) associated with said selected view to locate a match for said role (the roles authorization module retrieves the database entry for the requested resource using the URI and attempts to match a role from the userID-roles object with the roles in the roles/access database entry, see, e.g., col. 8, lines 1-4);

said locating step comprises the step of parsing a deployment descriptor (roles/access database, 422 in figure 4) for an application framework hosting said selected view and said different view to identify said set of roles (this is inherent process for authorization module 202 in figure 4, see, e.g., col. 7, line 53 to col. 8, line 11); and

said processing step comprises the step of invoking external access checking logic for a located server page tag referencing said access checking logic (this is inherent process for authorization module 202 in figure 4, see, e.g., col. 7, line 53 to col. 8, line 11).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles predefined.

Regarding claim 16, Bazinet teaches as follows:

A method for programmatic user privilege based security in a dynamically generated user interface (see, e.g., abstract), the method comprising the steps of:

configuring a deployment descriptor (portal generic objects database, 203 in

figure 2)(populating a portal generic object database, see, e.g., page 3, paragraph [0032]); and

composing a server page to include a reference to said external access checking logic and to invoke said external access in order to conditionally incorporate a link to a specific view associated with a specific set of authorized roles (the portal application, 102 in figure 1 and 502 in figure 5, generates a page to the client containing entries corresponding to the backend applications, see, e.g., page 3, paragraph [0038]).

Vasandani teaches as follows:

providing role based access security within a networked computing system (see, e.g., col. 2, lines 40-43);

the method for providing an authentication and authorization pipeline having a userID-roles database and a resource-roles database for use in a web server to grant access to web resources to users (see, e.g., col. 2, line 58 to col. 3, line 9); and

programming external access checking logic to match a parameterized role (userID-roles object, 211 in figure 4) with a role disposed in said set of roles in said deployment descriptor (roles/access database, 422 in figure 4)(the roles authorization module retrieves the database entry for the requested resource using the URI and attempts to match a role from the userID-roles object with the roles in the roles/access database entry, see, e.g., col. 8, lines 1-4).

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Bazinet to include the method of role based security access as taught by Vasandani in order to efficiently control security access by the user's roles

predefined.

Regarding claim 17, Bazinet teaches as follows:

said access checking logic is programmed to display said linkage where a role of the end user accessing said first view is authorized to access said second view (the portal application generate a page (equivalent to applicant's said linkage) to the client containing entries corresponding to the backend applications that the authenticated user can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraphs [0038] and [0039]).

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bazinet et al. (hereinafter Bazinet)(U.S. Pub. No. 2003/0167298 A1) and Vasandani et al. (hereinafter Vasandani)(U.S. Patent No. 6,985,946 B1) as applied to claim 4 above, and further in view of Schenk (U.S. Pub. No. 2006/0004887 A1).

Regarding claim 5, Bazinet and Vasandani teach all the limitations of claim 4 as explained above except for using Struts framework as the application framework incorporating the JSPs.

Schenk teaches as follows:

a configuration file is used to configure the presentation of an object (see, e.g., page 2, paragraph [0015]); and

Java server pages can be generated with Struts framework, as open source framework of utilizing pre-stored design patterns (see, e.g., page 2, paragraph [0017], lines 15-19).

It would have been obvious for one of ordinary skill in the art at the time of the

invention to modify Bazinet and Vasandani to include Struts framework as an application framework incorporating the JSPs as taught by Schenk in order to facilitate the development of JSPs applications.

Response to Arguments

5. Applicant's arguments filed 12/4/2007, with respect to claims 4-17 have been fully considered but they are not persuasive.

A. Summary of Applicant's Arguments

In the remarks, the applicant argues as followings:

1) Regarding claim 4, applicant is unclear what teaching within Bazinet identically discloses the "second view." Applications are not necessarily views;

2) Regarding claim 4, "access checking logic disposed in said first view and programmed to omit said linkage, the Examiner merely stated "no access." In this regard, applicant is entirely unclear how Bazinet teaches the specifically claimed limitations. A user having "no access" does not necessarily require that the linkage is omitted. Moreover, the Examiner has failed to establish that the access checking logic is disposed in the first view;

3) Regarding claim 4, the Examiner's assertion that it would have been obvious to include role based security access has no apparent relationship to whether or not linkage is omit in a first view, as claimed. In this regard, the Examiner has not explained why one having ordinary skill in the art would employ role based security access to this function. Moreover, Bazinet already teaches that the user is authenticated. In this regard, the Examiner has not explained why one having ordinary skill in the art would

modify Bazinet "to efficiently control security access" when security access has already been taught as being controlled by Bazinet; and

4) Regarding claims 8 and 12, the Examiner relied extensive upon Fig. 4 of Bazinet. For example, regarding the claimed "processing said selected view to identify a method call to access checking logic," the Examiner cited steps 422-434 in Fig. 4. However, these steps do not "identify a method call to access checking logic," as claimed.

B. Response to Arguments:

In response to argument 1), Bazinet teaches as follows:

the portal application generate a page (equivalent to applicant's first view) to the client containing entries corresponding to the backend applications (equivalent to applicant's first view) that the authenticated user can access based on the access privileges of the authenticated user (see, e.g., page 3, paragraph [0038] and step 416 in figure 4); and

linkage to the backend applications (124-130 in figure 1) is interpreted as the applicant's second view (by clicking the linkage (hyperlink) to the backend applications the second view inherently opens for the authenticated user, see, e.g., page 1, paragraph [0004]);

In response to argument 2), Bazinet teaches as follows:

The access checking logic (processing of checking authentication, 406-414 in figure 4) disposed in the portal application (102 in figure 4) and, the portal application provides the first view to the client (the portal application generate a page (equivalent to

applicant's first view) to the client, see, e.g., page 3, paragraph [0038] and step 416 in figure 4); and

access checking logic disposed in said first view and programmed to omit said linkage (the portal application generate a page (equivalent to applicant's first view) to the client containing entries corresponding to the backend applications that the authenticated user can access based on the access privileges of the authenticated user, see, e.g., page 3, paragraphs [0038] and [0039])(the web browser displays on page (502 in figure 5) a list of backend applications allowed for the authenticated user, which means inherently do not show backend applications (application p, data 4, 510 in figure 5) for the unauthenticated user (user i, 504 in figure 5), see, e.g., page 4, paragraph [0040] and figure 5);

In response to argument 3), In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Bazinet teaches the access control by authentication information (the authentication information includes user name and password combination, data on a smartcard etc, see, e.g., page 3, paragraph [0037]). Vasandani teaches the deficiency of role based access control (a userID-role database and a resource-role database for

use in a web server to grant access to web resources to users, see, e.g., col. 2, lines 58-62), though it is obvious to include the user roles in the authentication information.

In this case, the obviousness can be established by modifying the authentication information taught of Bazinet to produce the claimed invention in the knowledge generally available to one or ordinary skill in the art; and

In response to argument 4), Bazinet teaches as follows:

The portal application generate a page (equivalent to applicant's first view) to the client based on the checking authentication process (equivalent to applicant's access checking logic, 406-414 in figure 4)(see, e.g., page 3, paragraph [0038] and step 416 in figure 4).

Therefore, Bazinet inherently teaches a process of the page to identify with the checking authentication process.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

NATHAN FLYNN
SUPERVISORY PATENT EXAMINER

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeong S. Park whose telephone number is 571-270-1597. The examiner can normally be reached on Monday through Friday 7:00 - 3:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JP

February 6, 2008